

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

LAUNIUS MARKETING)
SPECIALISTS, INC.,)
)
 Plaintiff,)
)
)
vs.) Case No. 15-cv-1042-MJR-PMF
)
)
DAVID PEPPER, and)
APEX SALES &)
MARKETING, INC.,)
)
)
 Defendants.)

MEMORANDUM AND ORDER

REAGAN, Chief District Judge:

Launius Marketing Specialists is a sales company that serves as a middleman between automotive and industrial manufacturers and retail purchasers. It negotiates pricing agreements between those manufacturers and their retail buyers; handles retail orders; and coordinates pricing policies, collecting commissions for its work along the way. The information it generates is purportedly valuable in the trade, so Launius Marketing keeps it secret from its competitors. David Pepper is a former sales and marketing representative of Launius Marketing who left the company in July 2015 to work at his own competing business, which Pepper named Apex Sales & Marketing. Launius Marketing claims that Pepper looted files from the company's computers prior to his departure and is using those files in competition with Launius at Apex, and has sued Pepper and his company for violations of the federal Computer Fraud and Abuse Act and for other trade violations under Illinois law. Pepper and Apex Sales, for their

part, have moved to dismiss, claiming that the federal claim is bunk and that the Court shouldn't exercise supplemental jurisdiction over the attached state law claims. Apex Sales also claims that the complaint doesn't include any allegations directed at it, and thus it lacks the notice needed to respond under the federal rules.

Pepper was hired by the owner of Launius Marketing, William Launius, Sr., in May 2013. His job was to interface with Launius Marketing's existing manufacturer clients—he was responsible for meeting with those clients on a regular basis, handling complaints, and coordinating retail orders between the retailers and the manufacturers. Pepper evidently enjoyed the work and the relationship between Pepper and Launius blossomed—they got along so well that Pepper approached Launius during his first year at the company and expressed an interest in buying the company from Launius when he retired. Launius thought the sale made sense, so he began tutoring Pepper about the company and the two engaged in long-term talks about a transfer. From 2013 to 2015, Launius gave Pepper access to a great deal of the company's trade information so that he could do his job, and he gave Pepper access to the rest as a part of the sales negotiations process. The last time that Pepper and Launius met to discuss the sale was in July 2015. Rather than buy the business as planned, though, Pepper resigned from Launius Marketing on July 21, 2015, leaving to work at Apex Sales.

The sudden departure (and some gossip from another employee at Launius' company) made Launius suspicious, so he hired a forensic team to check his computers. The team allegedly discovered that Pepper had been digging through Launius Marketing's files in the months leading up to his departure. Pepper purportedly

transferred hundreds of Launius' computer files from the company's computer to his own personal cloud storage from January to March 2015; emailed himself Launius Marketing's customer lists from his Launius account to an Apex Sales account on April 30, 2015; accessed and possibly transferred more customer and sales documents on July 17, 2015; and deleted around one-hundred files on the day of his resignation. Those discoveries led to Launius' federal complaint and the defendants' motion to dismiss.

The motion to dismiss focuses on the Computer Fraud and Abuse Act claims, so the Court will start there. The Computer Fraud and Abuse Act is mainly a criminal statute, providing for imprisonment and fines for defendants who engage in certain types of hacking activities (like procuring government files without authorization, obtaining information from a protected computer without authorization, illegally trafficking in computer passwords, and so on). That said, the Act also provides a civil remedy for entities exposed to the hacking activities criminalized by the statute, so long as the entity suffered "damage" or "loss" "by reason" of those hacking activities and the hacking caused certain types of harms. *See 18 U.S.C. § 1030(g).* While Launius Marketing's complaint didn't specify what statutory "hacking" activities Pepper engaged in, the briefing clears things up—Launius says that Pepper exceeded his authorized access to Launius' protected computers to obtain information from them, in violation of **18 U.S.C. § 1030(a)(2)(C)**, and exceeded his authorized use of Launius' computers and obtained something of value from them in furtherance of a fraud, in violation of **18 U.S.C. § 1030(a)(4)**. Launius also says that those acts caused it "loss" because it had to hire an examiner to determine the extent of Pepper's pillaging.

Pepper and Apex first insist that the federal computer claims must be dismissed because one paragraph of the complaint was alleged on information and belief. The part at issue says that Pepper, on Launius' "belief," intentionally deleted Launius' files and intentionally accessed stored information. This argument is a bit undeveloped, as Pepper doesn't say whether the allegation in question needs more developed pleading under Federal Rule of Civil Procedure 9 or whether the laxer requirements of Federal Rule of Civil Procedure 8 apply. The distinction matters. For a complaint governed entirely by Rule 8, allegations made on information and belief are usually fine, so long as the complaint as a whole lays out enough facts to put the defendant on notice of the claim. *E.g., Arista Records, LLC v. Doe 3*, 604 F.3d 110, 119-20 (2d Cir. 2010); *Caroll v. Morrison Hotel Corp.*, 149 F.2d 404, 406 (7th Cir. 1945); *Trustees of the Auto. Mechs. Indus. Welfare & Pension Funds Local 701 v. Elmhurst Lincoln Mercury*, 677 F. Supp. 2d 1053, 1054-55 (N.D. Ill. 2010). Things are trickier in the Rule 9 context—certain fraud-related facts must be pled with more detail, and "information and belief" type allegations are only permitted when the fraud-related facts aren't in the possession of the plaintiff. *Pirelli Armstrong Tire Corp. v. Walgreen Co.*, 631 F.3d 436, 442-43 (7th Cir. 2011). Because Pepper and Apex make no mention of Rule 9 and make no argument concerning any failure to plead with particularity, the Court will assume that their argument is premised on Rule 8 rather than Rule 9. And because the complaint provides plenty of background about how Pepper accessed files, the single "information and belief" allegation linked to that point doesn't run afoul of Rule 8.

Pepper and Apex go on to argue that the federal claims must be dismissed because Launius Marketing hasn't properly alleged "damage" or "loss" for either of its unauthorized use claims. "Damage" and "loss" have special statutory meanings under the Computer Fraud and Abuse Act. The Act defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." **18 U.S.C. § 1030(e)(8).** "Loss," on the other hand, is "any reasonable cost to any victim," including "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information" to its past condition. **18 U.S.C. § 1030(e)(11).**

It's debatable whether Pepper's alleged deletions and downloading caused any statutory "damage" to Launius' files—the complaint doesn't say that the files were permanently deleted or impaired during Pepper's purported looting, just that some files were improperly accessed and others were improperly removed. That said, a party can state an "unauthorized use" claim under **18 U.S.C. § 1030(a)(2)(C)** or a "fraudulent use" claim under **18 U.S.C. § 1030(a)(4)** by alleging "loss" alone, so there's no need for the Court to deeply probe the "damage" question if "loss" has been pled. *See Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 768 (N.D. Ill. 2009) (collecting cases). It has. Launius Marketing says that Pepper deleted and improperly copied numerous files prior to his resignation from the company, that Launius had to hire an examiner to determine the depth of improper access, and that it spent more than \$5,000 for that examination. That's the kind of "loss" contemplated by the plain language of the Consumer Fraud and Abuse Act. *E.g., Farmers Ins. Exchange v. Auto Club Group*, 823 F. Supp. 2d 847, 854 (N.D. Ill. 2011); *Lemko Corp.*, 609 F. Supp. 2d at 768.

Pepper and Apex also claim that Launius' unauthorized use claims must fail because Pepper was authorized to access Launius' files. But the extent of Pepper's authorization, and when that authorization may have ended, are open questions for now. It's true that the complaint alleges that Pepper was given unfettered access to Launius Marketing's business information and files so that he could do his job and consider buying the business, but the complaint also alleges that Pepper breached his duty of loyalty to Launius and that the breach started before he departed the company and before he transferred or deleted files. That kind of allegation might not be enough to bring an unauthorized use claim in those circuits that adopt a narrower view of the term "unauthorized," *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1137 (9th Cir. 2009), but the Seventh Circuit hasn't bought into that view. To the contrary, it has held that an employee's computer use can become unauthorized once there is a "serious breach of loyalty to the principal," as the breach destroys the agency relationship and the authorizations conveyed with it. *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 421 (7th Cir. 2006). Launius alleges a breach of loyalty here, so the use claims can't be dismissed at this stage on the grounds that Pepper was given initial access to the files.

Pepper and Apex insist that there was no possible breach of loyalty—and thus no lack of authorization—because the complaint says that one of Launius Marketing's employees knew that Pepper was attempting to steal clients and compete with Launius in May or June of 2015. In their view, the breach of loyalty was sanctioned by that employee's knowledge, so Pepper's agency-given authorization was never terminated. Assuming that knowledge alone could excuse a serious breach of loyalty and keep an

agency relationship intact, and the comments to the **RESTATEMENT (SECOND) OF AGENCY § 112 (1958)** cast some doubt on that premise,¹ there are a few factual problems with the defendants' theory at this phase of the case. For one, the complaint says that Pepper started transferring files before May 2015, and there's no indication that anyone at Launius Marketing knew of (and authorized) Pepper's purported subterfuge at that time. More fundamentally, the employee who knew of Pepper's acts was Launius' receptionist and office manager, and not William Launius himself, the person alleged to be the principal of Launius Marketing. It's the knowledge of the principal that matters for purposes of the agency relationship, *Citrin*, 440 F.3d at 421, and there's nothing in the complaint to indicate that Launius' receptionist was the principal here.

That takes care of all of the arguments jointly advanced by Pepper and Apex Sales, leaving only Apex Sales' argument that none of the claims in the complaint are specifically directed at Apex, and thus it lacks sufficient notice of the claims against it (presumably under Federal Rule of Civil Procedure 8). While it's a close question, the Court is of the view that the complaint includes sufficient detail to clue Apex in to Launius' claims against it. The complaint says that Apex Sales was formed by Pepper, and that Apex "and/or" Pepper violated the Illinois Trade Secrets Act and the Computer Fraud and Abuse Act based on Pepper's conduct at Launius in the months leading up to his departure from the company and his conduct shortly thereafter. In other sections, the complaint lays out Pepper's improper access to files and his possible

¹ If Pepper and Apex wish to make this argument again once the factual record is more developed, they will need to offer more than a single undeveloped citation in support.

use of Launius' information at Apex. The complaint also says that Pepper transferred files to an Apex email account during his tenure at Launius, and it suggests that Pepper started to form Apex before leaving Launius. At this early point, the Court must accept all of the facts pled in the complaint as true and must draw all reasonable inferences from those facts in Launius' favor. The allegations in the complaint suggest that Pepper could have been acting more in an Apex capacity (and thus on Apex' directives) when he obtained files from Launius Marketing, and that Apex (through Pepper) could have improperly used Launius Marketing's files after Pepper left Launius. Launius could have done a better job of pleading its claims against Apex Sales, but the allegations are enough, if barely, to give Apex the notice required by Rule 8.

To sum up, Pepper and Apex' motion to dismiss the Computer Fraud and Abuse Act claims is **DENIED**, and because those claims remain, their motion to dismiss the remaining state law claims is **DENIED** as well. Apex' request to dismiss the entire complaint on the grounds that it doesn't provide adequate notice is also **DENIED**.

IT IS SO ORDERED.

DATED: May 23, 2016

/s/ Michael J. Reagan
Chief Judge Michael J. Reagan
United States District Court